DATA PROTECTION LAWS OF THE WORLD

Morocco

MOROCCO

Last modified 18 January 2024

LAW

Morocco’s law governing privacy and data protection is Law No 09-08, dated February 18, 2009 relating to protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of May 21, 2009 (together the DP Law).

DEFINITIONS

Definition of personal data

Pursuant to Article 1 of the DP Law, personal data is defined as any information regardless of their nature, and format, relating to an identified or identifiable person.

Definition of sensitive personal data

Sensitive personal data is defined under the law as personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs or union membership of the person concerned or relating to his health, including his genetic data (article 1.3 of the DP Law).

NATIONAL DATA PROTECTION AUTHORITY

The relevant authority is the Data Protection National Commission (*Commission Nationale de Protection des Données Personnelles*).

REGISTRATION

The processing of personal data is subject to:

- A prior declaration to be filed with the Moroccan Data Protection Commission; or
- A prior authorization of the Moroccan Data Protection Commission when the processing concerns any of the following:
    - Sensitive data (e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic data);
    - Using personal data for purposes other than those for which they were initially collected;
    - Genetic data, except for those used by health personnel and that respond to medical purposes;
    - Data relating to offenses, convictions or security measures, except for those used by the officers of the court;
    - Data which includes the number of the national identity card of the concerned person.

The declaration and authorization includes a commitment that the personal data will be treated in accordance with the DP Law.

The prior declaration and authorization shall include, without limitation, the following information:

- The name and address of the person in charge of the processing and, if applicable, its representative;
- The name, characteristics and purpose(s) of the intended processing;
- A description of the category or categories of data subjects, and the data or categories of personal data relating thereto;
- The recipients or categories of recipients to whom the data are likely to be communicated;
- The intended transfers of data to foreign states;
- The data retention time;
- The authority with which the data subject may exercise, if any, the rights granted to him / her by law, and the measures taken to facilitate the exercise of these rights;
- A description of the confidentiality and security measures in place to protect personal data; and
- Overlap, interconnections, or any other form of data reconciliation and their transfer, subcontracting, in any form, to third parties, free of charge or for consideration.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer under the DP Law.

COLLECTION & PROCESSING

The personal data must be processed in accordance with the following principles:

- Treated fairly and lawfully;
- Collected for specific, explicit and legitimate purposes;
- Adequate, relevant and not excessive;
- Accurate and necessary and kept up-to-date;
- Kept in a form enabling the person concerned to be identified.

As a general rule, the processing of a personal data must be subject to the prior consent of the relevant data subject.

While the applicable regulations provide that the processing of personal data can be performed without the consent of the relevant data subject in some specific instances, the Moroccan Data Protection Commission rarely accepts that the data controllers process personal data without the consent of the relevant data subject.

TRANSFER

Prior authorization from the National Commission is required before any transfer of personal data to a foreign state.

Further, the person in charge of the processing operation can transfer personal data to a foreign state only if the said state ensures under its applicable legal framework an adequate level of protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which these data is or might be subject, unless:

- The data subject has expressly consented to the transfer
- The transfer and subsequent processing is required for:
    - Compliance with a legal obligation to which the concerned person or the person in charge of the processing are submitted
    - The execution of a contract to which the concerned person is party or in the performance of pre-contractual measures taken at the request of the latter
    - The protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give its consent
    - Performance of a task of public interest or related to the exercise of public authority, vested in the person in charge of the processing or the third party to whom the data are communicated

- Fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the relevant data subject

In practice, we notice that CNDP interprets the exception of legitimate interests of the data processor very restrictively. CNDP is in general more comfortable relying on the data subject’s consent regarding any transfers to a foreign state.

SECURITY

Article 23 of the DP Law provides that an organization is required to implement all technical and organizational measures to protect personal data in order to prevent it being damaged, altered or used by a third party who is not authorized to have access, as well as to protect it against any form of illicit processing.

Additionally, in appointing processors and subcontractors an organization must choose a processor or subcontractor who provides sufficient guarantees with regard to the technical and organizational measures relating to the processing to be carried out while ensuring compliance with these measures.

BREACH NOTIFICATION

There is no requirement for a data protection officer under the DP Law, except, where relevant, through the application of GDPR.

ENFORCEMENT

The Data Protection National Commission enforces compliance of the DP Law.

Article 50 to 64 provide that non-compliance with the DP Law is punishable by a fine ranging from DH10,000 to DH600,000 and / or imprisonment between three months and four years.

If the offender is a legal person, and without prejudice to the penalties which may be imposed on its officers, penalties of fines shall be doubled.

In addition, the legal person may be punished with one of the following penalties:

- The partial confiscation of its property
- Seizure of objects and things whose production, use, carrying, holding or selling is an offense
- The closure of the establishment(s) of the legal person where the offense was committed

ELECTRONIC MARKETING

Direct marketing by means of an automated calling machine, a fax machine, email or a similar technology, which uses, in any form whatsoever, an individuals' data without their express prior consent to receive direct prospecting is prohibited.

However, direct marketing via email may be allowed if the recipient’s email address has been received directly from him / her.

In the absence of consent, unwanted emails can only be sent if all of the following conditions are satisfied:

- The contact details were provided in the course of a sale
- The marketing relates to a similar product

- The recipient was given a method to opt out of the use of their contact details for marketing when they were collected

ONLINE PRIVACY

The general data protection principles under the DP Law apply.

KEY CONTACTS

Mehdi Kettani
Head of IPT
T +212 (0) 660 16 44 56
Mehdi.Kettani@dlapiper.com

Adil Mouline
Lawyer
T +212 (0) 620 57 00 00
Adil.Mouline@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.